P1 1170753

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

May 19, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/454,542*
FILING DATE: *March 14, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/07403*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

M. Sias

M. SIAS
Certifying Officer

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

03-17-03 60454542.031403

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Express Mail Label No. EV 249512487 US

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
SACHIN S.	MODY	LAWRENCEVILLE, NJ
SAURABH	MATHUR	PLAINSBORO, NJ
JUNBIAO	ZHANG	BRIDGEWATER, NJ

☐ *Additional inventors are being named on the _____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

WLAN SESSION MANAGEMENT TECHNIQUES WITH SECURE REKEYING AND LOGOFF

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number _____ *Type Customer Number here*

OR

Place Customer Number Bar Code Label here

☒ Firm or Individual Name	JOSEPH S. TRIPOLI, THOMSON LICENSING INC.				
Address	PATENT OPERATIONS.				
Address	P. O. BOX 5312				
City	PRINCETON	State	NJ	ZIP	08543-5312
Country	USA	Telephone	609-734-6834	Fax	609-734-6888

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 2 ☐ CD(s), Number _____

☐ Drawing(s) *Number of Sheets* _____ ☐ Other (specify) _____

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 07-0832

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($): 160

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____.

Respectfully submitted, SIGNATURE Paul P. Kiel	Date: 3/14/03
TYPED or PRINTED NAME PAUL P. KIEL	REGISTRATION NO. 40,677 *(if appropriate)*
TELEPHONE 1 609 734 6815	Docket Number: PU030081

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C., 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Express mail: EV 249512487 US PU030081

WLAN SESSION MANAGEMENT TECHNIQUES WITH SECURE REKEYING AND LOGOFF

This invention describes a scheme in which a wireless LAN (WLAN) user can maintain a secure session with the WLAN with periodic key update and secure logoff. Compared with existing session management mechanisms such as IEEE 802.1x, our mechanism has the following advantages:

- It does not require an authentication server for key update. This is particularly useful when the authentication server is far away, such as in the WLAN-3G interworking scenario where it is desirable to limit the control traffic from the wireless user to the cellular network. It is also especially useful in application scenarios such as in a home environment, where an authentication server may not be available. Our mechanism would still allow key update to increase the security level.
- Management information, in particular, logoff requests, is exchanged in a secure manner. In IEEE 802.1x, such information is sent in the clear. It is thus prone to attacks in which a hacker can logoff an authenticated user even though the hacker does not have the session key.
- It is particularly useful in web browser based public WLAN hot spot access solutions such as the one proposed in [1].

Once a user is authenticated by a WLAN, a secure session key is established and shared by the user and the WLAN. All subsequent communication will be encrypted using this session key. To prevent security attacks (e.g. attacks exploring security holes in the IEEE 802.11 WEP mechanism) and ensure strong security, the session key needs to be updated periodically. In IEEE 802.1x, the standard to be used for secure access control in WLANs, session key update relies on an authentication server. In essence, each time the key is updated, the user needs to go through the authentication steps similar to the initial authentication. As we discussed earlier, this can be quite inefficient in some cases and impossible in some application scenarios. In our scheme, once the user is authenticated and the session key is established, future key update no longer requires the participation of the authentication server.

Management information exchange

In our scheme, management information, such as key update or logoff requests, are encrypted with the same session key as the user data. Such information can be carried in special management frames or in regular data frames.

Key update

A simple form of local key update is to let the wireless user or the WLAN AP periodically (or based on the number of communicated frames/packets) initiate key refresh. Both the WLAN AP and the wireless user agree on a new key and start using this key. Since the key update communication between them is encrypted with the old key that is not known to an attacker, the new key should also be unknown to the attacker. However, this is based on the assumption that the old key is secure. If for some reason

the old key is cracked by a hacker (e.g. the key update is not frequent enough), the hacker can then know all the subsequent keys. This is rather undesirable.

To solve this problem, we use the following scheme:

- During the user authentication phase, instead of installing one shared secret -- the initial session key -- on both the wireless user machine and the WLAN AP, two shared secrets are installed. One of them is used as the initial session key, the other is used as a secure seed. Since the initial authentication is secure, these two keys are not known to the attacker. The initial session key may eventually be cracked by the attacker. For example, if the initial session key is used as a WEP key, after certain number of communication exchanges using the WEP key between the wireless user and the WLAN AP, the attacker may crack the key. However, the secure seed remains secure as it is not used in any insecure communication.
- When a key update is necessary, a new key is generated and exchanged between the WLAN AP and the wireless user. Instead of directly using this new key, the AP and the wireless user use this new key together with the secure seed to generate the new session key. For example, the new session key may be generated by concatenating the secure seed with the new key, and then run MD5 hash algorithm to generate a fixed string. Other mechanisms can also be used. Since the attacker does not have the secure seed, even if he can crack the old session key, he won't be able to get the new session key

Secure logoff

As we discussed earlier, session logoff must be secure to prevent an attacker from logging off authenticated users. The IEEE 802.1x based scheme cannot provide secure logoff because the logoff request is carried in an unencrypted frame. In our scheme, the wireless user sends the logoff request as encrypted traffic. Further, the logoff request is accompanied by the secure seed. Thus even if the attacker cracks the session key, he still could not log off the authenticated user. Since the secure seed appears in the logoff request and will no longer be used (a new secure seed needs to be negotiated each time the user logs in), thus even if it is seen by the attacker, no harm can be done.

Conclusion

The proposed mechanism provides secure wireless session with secure local key update and secure logoff. These features are not available in the current wireless LAN solutions such as IEEE 802.1x. They provide low-overhead, strong security solutions to all kinds of wireless LAN environment, from homes, enterprises, to public WLAN hot spots.

References:

[1] IU020369, Junbiao Zhang, Saurabh Mathur, Kumar Ramaswamy, "A WEB BROWSER BASED HOT SPOT WLAN ACCESS SOLUTION WITH STRONG SECURITY"

[redacted]